基于明文相关的混沌映射与 SHA-256 算法的数字图像的加密与监测 *

刘西林，严广乐

(上海理工大学 管理学院，上海 200093)

摘 要：针对数字图像的传播安全性问题，以及数字图像加密脱离明文，过分依赖混沌系统的问题，提出了基于明文相关的混沌映射与 SHA-256 算法的数字图像的加密与监测算法。算法通过使用 SHA-256 算法计算明文图像的哈希值，作为摘要来监测数字图像的传播；使用前向扩散、关联明文的置乱与后向扩散的方法对数字图像进行加密，Lorenz 混沌映射产生相应的密码。结果表明该算法具有较好的抵抗各种攻击的能力，达到了图像传播的安全性与隐蔽性的目的。

关键词：混沌系统；图像加密；SHA-256；哈希值；Lorenz 混沌映射

中图分类号：TP309.7   doi: 10.3969/j.issn.1001-3695.2018.07.0411

Encryption and monitoring of digital images based on plaintext related chaotic map and SHA-256 algorithm

Liu Xilin, Yan Guangle

(*Business School*, *University of Shanghai for Science& Technology*, *Shanghai* 200093, *China*)

Abstract: For the security problem of the spread of digital image and the digital image encryption from plaintext and too depend on the chaotic systems, this paper proposes a digital image encryption and monitoring algorithm combined with plaintext-related chaotic mapping and SHA-256. The algorithm uses the SHA-256 algorithm to calculate the hash value as record to monitor the spread of digital image; Lorenz chaotic mapping generates the corresponding cryptogram by using forward diffusion, associated plaintext scrambling and backward diffusion to encrypt the digital image. The results show that the algorithm can resist many attacks and achieve the security and concealment of image propagation.

Key words: chaotic systems; image encryption; SHA-256; hash value; Lorenz chaotic mapping

0 引言

随着网络信息技术的迅速发展，在通信系统的传输过程中，数字图像信息极其容易被恶意者拦截，面临着隐私泄露和数据安全等问题。在远程医疗、军事、个人图像、视频会议和生物指标系统等应用中，图像的传输需要确保安全性，但泄露事件却频有发生错误!未找到引用源。。因此，数字图像的加密是数字图像安全传输的重要保障。

伴随着人们越来越重视数字图像传输中的安全性问题，近年来学者们提出了一些新的图像加密算法错误!未找到引用源。。其中有基于图像像素点位置置乱与像素值扩散的如文献[2~4]，都完成了数字图像的加密，但都存在着密钥空间小的问题。文献[5,7,8]都是基于数字图像的频域变换与混沌系统结合，使得将数字图像能完成更好的加密效果，但同时存在加密后密文图像信息熵偏小的问题。而文献[4]将多个方法与混沌系统结合对数字图像进行加密，算法密钥空间很大，但加密解密过程繁琐，存在效率低的问题。此外，以上的部分文献算法还存在置乱与扩散严重依赖混沌系统，脱离明文，从而削弱了算法的可靠性问题。在众多经典的数字图像密码系统中，密钥是产生加密明文图像的密码的唯一依据，即密码仅受密钥控制，与密钥有关，而与明文无关，这种类型的图像密码系统易受选择明文攻击或已知明文攻击错误!未找到引用源。。

为此，本文提出了基于明文相关混沌映射与 SHA-256 算法的数字图像的加密与检测。首先通过对数字图像的灰度图像使用 SHA-256 算法生成 256bit 的哈希值作为摘要，来监测密文图像在传播过程中是否被篡改；其次，使用前向扩散与逆向扩散相结合的方法对数字图像的像素值进行扩散，使用明文相关的置乱算法对数字图像的位置进行置乱后形成密文，即密码的生成不止与密钥有关还和明文的信息有关；三维 Lorenz 混沌映射产生对应的密码。这样传输加密后的图像就实现了数字图像的隐秘传输。实验结果显示该算法不仅能够提高密钥的敏感性、监测传输图像的安全性，还能有效的抵抗明文、暴力等其他攻击。

收稿日期：2018-07-09；**修回日期：**2018-08-31 **基金项目：**上海高原学科建设项目（10-17-303-004）

作者简介：刘西林（1992-），男，硕士研究生，主要研究方向为混沌加密、图像处理（745834896@qq.com）；严广乐（1957-），男，教授，博士，主要就主要研究方向为混沌系统、系统科学与复杂网络.

1　SHA-256 算法、混沌系统

1.1　SHA-256 算法

SHA(secure hash algorithm)安全加密标准，是至今国际上使用最为广泛的较为安全的压缩算法之一，由美国 NIST 和 NSA 两个组织共同开发的，此算法于 1993 年 5 月 11 日被美国 NIST 和 NSA 设定为加密标准错误!未找到引用源。。SHA-256 算法就是其中一个，该算法弥补了 SHA-1 存在安全隐患的问题。可以将数字图像信息转换成 256 bit 的哈希值，数字图像内容有任何微小的变换，哈希值都会发生巨大的变化，经使用 SHA-256 算法的数字图像，就相当于拥有了“指纹”。

1.2　Lorenz 混沌系统

本文采用的是 Lorenz 系统映射，其具体的动力学方程如下所示：

$$\begin{cases} x = a(y-x)+w \\ y = cx - y - xz \\ z = xy - bz \\ w = -yz + rw \end{cases} \tag{1}$$

其中:a，b，c，w，r 为超混沌系统的参数，x, y, z 为 Lorenz 混沌系统产生混沌序列的三个状态变量，当 a=10，b=8/3，c=28，$-1.52 \le r \le -0.06$ 时，式（1）处于混沌状态错误!未找到引用源。。

2　加密方案设计

方案设计流程图如图 1 所示。

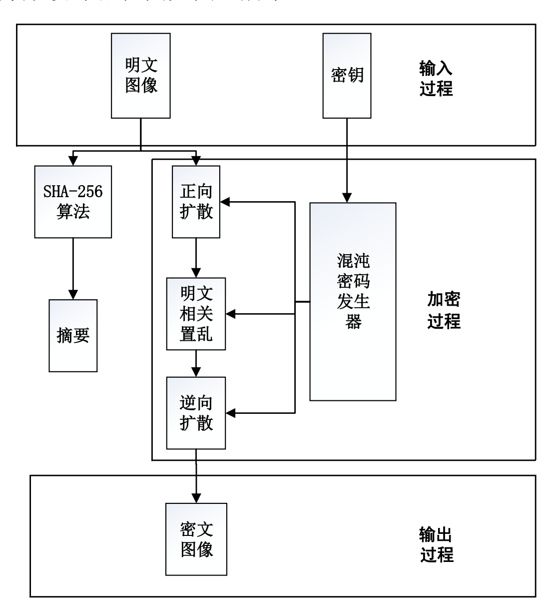


图 1　方案设计流程图

2.1　产生图像摘要

将数字图像转换成灰度图像，即三维矩阵转换成二维矩阵(不可逆)。将灰度图像经过 SHA-256 算法产生的 256bit 哈希值作为摘要，成为数字图像的“指纹”，对经典 Lena 灰度图像使用 SHA-256 算法编码产生的 256 位摘要(哈希值)为：9a9b4963ddaa149de2d7d66b5c952e2fe0036f4a819046998f766be605eb3f18。发送方保存该摘要值等待与接收方解密密文后再经过 SHA-256 编码的摘要值进行匹配。

2.2　图像加密

本文提出的加密算法首先对原始图像的像素值就行正向扩散操作；然后进行明文相关的置乱方法对像素的位置进行置乱操作；最后再进行逆向扩散像素值，形成密文。混沌 Lorenz 系统的参数和初始值作为密钥。解密过程是加密过程的逆过程。假设明文图像为 P，大小为 M*N，灰度等级为 L，密钥 $K=\{x_0,y_0,z_0,w_0,r_1,r_2\}$，其中 $\{x_0,y_0,z_0,w_0\}$ 为状态初值，r_1,r_2 为两个 8b 的随机数。具体加密步骤如下：

a)借助于密钥状态初值，迭代混沌 Lorenz 系统产生 4 个伪随机序列 $\{x_i\}$、$\{y_i\}$、$\{z_i\}$、$\{w_i\}$，i=1，2，⋯，MN。借助于这四个伪随机序列，生成矩阵 X、Y、Z、W、U 和 V。具体公式如下错误!未找到引用源。：

$$\begin{cases} X(k,l) = floor\left((x_{(k-1)*N+l} + 500 \bmod 1)*10^{13}\right) \bmod 2^L \\ Y(k,l) = floor\left((y_{(k-1)*N+l} + 500 \bmod 1)*10^{13}\right) \bmod 2^L \\ Z(k,l) = (floor(z_{(k-1)*N+l} *10^{13}) \bmod M) + 1 \\ W(k,l) = (floor((w_{(k-1)*N+l} + 500 \bmod 1)*10^{12}) \bmod N) + 1 \\ U(k,l) = (floor((x_{(k-1)*N+l} + y_{(k-1)*N+l} + 500 \bmod 1)*10^{12}) \bmod M) + 1 \\ V(k,l) = (floor((z_{(k-1)*N+l} + w_{(k-1)*N+l} + 500 \bmod 1)*10^{12}) \bmod N) + 1 \end{cases} \tag{2}$$

其中：k=1，2，⋯M; l =1，2，⋯N ； $floor(t)$ 返回小于等于 t 的最大整数。

b)将明文图像 P 通过正向扩散转换成矩阵 A，具体公式如下：

$$\begin{cases} A(i,j) = P(i,j) + X(i,j) + r_1 \bmod 2^L (i=1, j=1) \\ A(i,j) = P(i,j) + A(i,j-1) + X(i,j) \bmod 2^L (i=1, j=j+1, j \le N) \\ A(i,j) = P(i,j) + sum(A(i-1,1toN)) + X(i,j) \bmod 2^L (i=i+1, j=1, i \le M) \end{cases}$$

(3)

其中 $sum(t)$ 返回向量 t 中所有元素的和。

c)通过明文相关的置乱算法将图像矩阵 A 转换成矩阵 B，具体公式如下所示：

$$\begin{cases} m = U(i,j) + sum(A(Z(i,j),1toN) \bmod M) + 1 \\ n = V(i,j) + sum(A(1toM, w(i,j)) \bmod N) + 1 \end{cases} \tag{4}$$

其中 m 和 n 分别是矩阵 B 的坐标，在 m=i 或 Z（i，j），或者 n=j 或 $W(i,j)$, 或者 $Z(i,j)$=i 或者 $W(i,j)$=j 情况下，$A(i,j)$位置不变，否则 $A(i,j)$与 $A(m,n)$互换位置，$sum(t)$ 返回向量 t 中所有元素的和。

d)再对矩阵 B 进行逆向扩散得到矩阵 C，具体公式如下：

$$\begin{cases} C(i,j) = B(i,j) + Y(i,j) + r_2 \bmod 2^L (i=M, j=N) \\ C(i,j) = B(i,j) + C(i,j+1) + Y(i,j) \bmod 2^L (i=M, j=j-1, j>1) \\ C(i,j) = B(i,j) + sum(C(i+1,1toN)) + Y(i,j) \bmod 2^L (j=N, i=i+1, i \ge 1) \end{cases}$$

(5)

其中 $sum(t)$ 返回向量 t 中所有元素的和。

经过正向扩散，明文相关的置乱，逆向扩散可以得到密文

图像。

3　仿真实验

在 MATLAB 7.1 环境下对本文提出的算法进行仿真实验，得到结果。待加密的 Lena 图像如图 2 所示，加密后的 Lena 图像如图 3 所示，解密后的 Lean 灰度图像如图 4 所示，错误密钥解密后的图像如图 5 所示，待加密的 Cameraman 图像如图 6 所示，加密后的 Cameraman 图像如图 7 所示，正确秘钥解密后的 Cameraman 图像如图 8 所示，错误秘钥解密后的图像如图 9 所示。


图 2　待加密的 Lena 图像

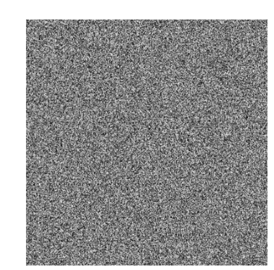

图 3　加密后的密文图像


图 4　解密后的 Lena 图像

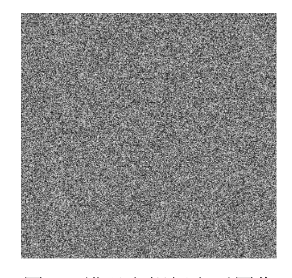
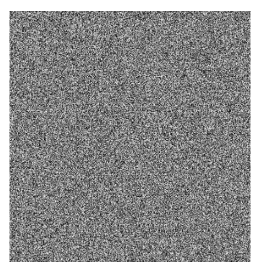
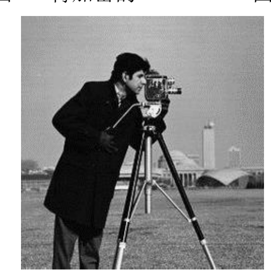
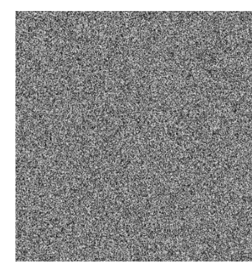

图 5　错误密钥解密后图像


图 6　待加密的 Cameraman 图像


图 7　加密后的密文图像


图 8　正确秘钥解密后的图像


图 9　错误秘钥解密后的图像

接收方解密 Lena 后的图像再经过使 SHA-256 算法编码产生的摘要（哈希值）为：9a9b4963ddaa149de2d7d66b5c952e2fe0036f4a819046998f766be605eb3f18，若在图像传播过程中图像信息被稍微改动使用 SHA-256 算法编码为：44b8ca7c15500098ad801b4c96d4237fa54685594a55924cff8e1a296818b313。

接收方解密 Cameraman 后的图像再经过使 SHA-256 算法编码产生的摘要（哈希值）为：29c69af72fd1e6f6b1e7603573a2b750e11a30480516af6ea34f17ef0caf2021，若在图像传播过程中图像信息被稍微改动使用 SHA-256 算法编码为：345f41ccf15e39e6f2271155fd0cbd465da0a66151f4273a8a71f7816add2e13。

接收方的摘要值与发送方的摘要值进行匹配，发现有差异，说明图像在传播过程中存在被篡改的行为；没有差异，说明图像传输过程中安全。

4　安全性分析

4.1　直方图分析

数字图像的加密可以将明文转换成噪声从而隐藏信息。直方图可以表现图像像素的分布频率，描述图像的统计相关性。一般情况下，图像像素灰度的直方图越服从均匀分布，越能有效的抵抗统计分析的攻击。以经典图像 Lena 为例：加密前图像的灰度直方图如图 10 所示，加密后的灰度直方图如图 11 所示。从图可以看出加密后的图像灰度直方图更接近于均匀分布，说明加密后能有效地抵抗统计分析的攻击。

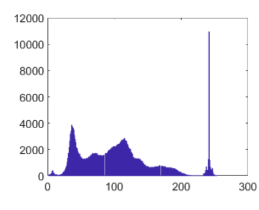


图 10　加密前灰度直方

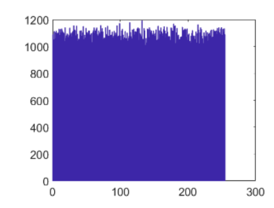


图 11　加密后灰度直方图

4.2　相关性分析

明文图像相邻像素之间有很强的相关性，而这些相关性内部存在着明文的部分信息，若被不法分子发现利用，很可能会造成图像的泄露错误!未找到引用源。。优良的加密算法能使得图像的像素之间的相关性变弱。本文从待加密的 Lena 图像与加密后的密文图像中分别随机挑选了 2000 对相邻的像素点，描绘出他们各个方向的相关性图像如图 12 所示，计算出各个方向的相关系数如表 1 所示。从图与表可以看出，加密后的图像相邻像素点的相关性明显降低，使图像更加安全。相关系数的计算公式为：

$$
\begin{aligned}
r_{xy} &= \frac{\operatorname{cov}(u,v)}{\sqrt{D(u)}\sqrt{D(v)}} \\
\operatorname{cov}(u,v) &= \frac{1}{N}\sum_{i=1}^{N}\left(x_i - E(u)\right)\left(y_i - E(v)\right) \\
D(u) &= \frac{1}{N}\sum_{i=1}^{N}\left(u_i - E(u)\right)^2 \\
E(u) &= \frac{1}{N}\sum_{i=1}^{N}u_i
\end{aligned}
\tag{5}
$$

其中 N 为任取的相邻像素点的对数，他们的灰度值为 (u_i, v_i)，i=1，2，⋯N，向量 $u=\{u_i\}, v=\{v_i\}$。

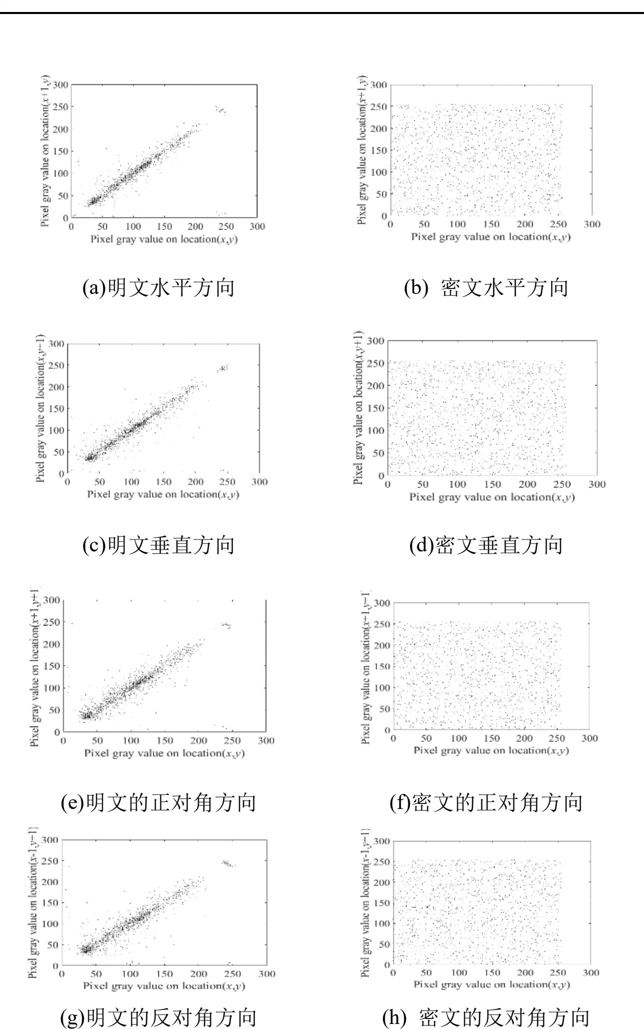

(a)明文水平方向　(b) 密文水平方向
(c)明文垂直方向　(d)密文垂直方向
(e)明文的正对角方向　(f)密文的正对角方向
(g)明文的反对角方向　(h) 密文的反对角方向

图 12　相关性图像

表 1　相关系数

图像	水平	垂直	正对角	反对角
明文	0.9438	0.9354	0.8856	0.8875
密文	0.0220	0.0272	-0.0244	0.0308

4.3　信息熵计算

信息熵反应图像不确定性，一般情况下，算法的加密效果越好，图像的信息熵越大，图像的信息量和随机性也越大。几个文献加密经典 Lena 图像的信息熵结果如表 2 所示。信息熵的具体公式如下：

$$H=-\sum_{i=0}^{L}p(i)\log 2p(i) \tag{6}$$

其中 L 为图像灰度等级数，P(i)表示灰度值 i 出现的概率。

对于 L=256 的灰度图像，信息熵 H 理论值为 8.由表中数据可以发现，虽然文献[1]和文献[3]以及本算法的信息熵都很接近，但本算法加密后的 Lena 图像的信息熵更接近于 8，说明本算法更能有效地抵抗数据攻击[错误!未找到引用源。]。

表 2　信息熵结果

图像	信息熵值
Lena 明文图像	7.3804
本算法的密文图像	7.9994
文献[1]的密文图像	7.9968
文献[6]的密文图像	7.9897

4.4　密钥空间分析

密钥空间是指所有合法密钥的集合，加密算法越好，则相应的密钥空间越大[错误!未找到引用源。]。本文密钥 $K=\{x_0,y_0,z_0,w_0,r_1,r_2\}$，其中，$x_0\in(-40,40)$，$y_0\in(-40,40)$，$z_0\in(1,81)$，$w_0\in(-250,250)$，其中 x_0、y_0 和 z_0 的步长为 10^{-13}，w_0 的步长为 10^{-12}，r_1 和 r_2 为 0~255 的整数，可得密钥空间大约为 $1.6777*10^{64}$，约为 213 比特，而文献[2]的密钥空间只有 $(10^{16})^2$，虽然本算法的密钥空间大，但平均加密速度在 14~20 s 之间，而文献[2]的平均加密速度在 10 秒左右，文献[4]的平均加密速度在 30 秒以上。综合以上分析，在平均加密速度稍快的情况下，本算法的密钥空间更大，更能抵抗暴力攻击。

4.5　差分攻击分析

像素改变率(NPCR)和归一化平均改变度(UACI)是衡量图像加密算法抵抗差分攻击能力的重要指标[错误!未找到引用源。]。差分攻击是指对明文稍微改变，再进行加密，比较相应前后密文的差异，若前后密文相差较大，则说明该算法有较强的抗明文攻击和差分攻击的能力。本算法的重复 100 次试验的 NPCR 和 UACI 的平均值值如表 3 所示。NPCR 和 UACI 的具体公式如下：

$$NPCR(P_1,P_2)=\frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}\left|Sign\left(P_1(i,j)-P_2(i,j)\right)\right|*100\%$$

其中

$$Sign(x)=\begin{cases}1, x>0\\0, x=0\\-1, x<0\end{cases} \tag{7}$$

$$UACI(P_1,P_2)=\frac{1}{MN}\sum_{i}^{M}\sum_{j}^{N}\frac{\left|P_1(i,j)-P_2(i,j)\right|}{255-0}*100\% \tag{8}$$

其中:M 和 N 分别是图像的长度和宽度，$P_1(i,j)$ 和 $P_2(i,j)$ 分别指明文改变前后的密文像素值。

表 3　NPCR 和 UACI 的测试结果　/%

指标	Lena 密文	理论值
NPCR	99.6085	99.6094
UACI	33.4576	33.4635

由表 3 可知本算法加密像素稍微改变的明文，密文相差很大，NPCR 和 UACI 的值很接近它们的理论值，说明该算法有较好的抗明文攻击与差分攻击的能力。

5　结束语

本文提出了一种基于明文相关的混沌映射与 SHA-256 算法的数字图像的加密与监测。首先对待加密图像的灰度图像使用 SHA-256 算法编码产生的哈希值作为摘要来监测密文图像在传输过程中是否被篡改。使用两次不同的扩散方法以及明文相关的置乱算法对数字图像就行加密，Lorenz 混沌映射产生对应的密码。实验结果表明，该算法不仅密钥空间大，而且能够有效的抵抗暴力攻击、明文攻击、统计攻击与差分攻击，从而更好的保障了数字图像的安全传输。

参考文献：

[1] 韩栋，王春华，肖敏. 基于混沌映射和二次剩余密码的彩色图像加密方法 [J]. 计算机应用研究, 2018, 35 (9): 2757-2761. (Han Dong, Wang Chunhua, Xiao Min. Color image encryption method based on chaotic map and quadratic residue cryptosystems [J//OL]. Application Research of Computers, 2018, 35 (9): 2757-2761.)

[2] 李春虎，罗广春，李春豹. 基于斜帐篷混沌映射和 Arnold 变换的图像加密方案 [J/OL]. 计算机应用研究, 2018, 35 (11) . (2017-11-10) [2017-11-10]. http://www. arocmag. com/article/02-2018-11-028. html. (Li Chunhu, Luo Guangchun, Li Chunbao. Image encryption scheme based on skew tent chaotic map and Arnold transformation [J/OL]. Application Research of Computers, 2018, 35 (11) . (2017-11-10) [2017-11-10]. http://www. arocmag. com/article/02-2018-11-028. html.)

[3] 蒋君莉，张雪锋. 基于多混沌系统的彩色图像加密方法 [J]. 计算机应用研究, 2014, 31 (10): 3131-3136. (Jiang Junli, Zhang Xuefeng. Color image encryption method based on chaotic system [J]. Application Research of Computers, 2014, 31 (10): 3131-3136.)

[4] 孙力，黄正谦，梁立. 基于复合混沌映射与连续扩散的图像加密算法 [J]. 计算机工程与设计, 2017, 38 (12): 3374-3379. (Sun li, Huang Zhengqian, Liang Li. Image encryption algorithm based on composite chaotic maps and continuous diffusion [J]. Computer Engineering and Design, 2017, 38 (12): 3374-3379.)

[5] 闫兵，柏森，刘博文，等. 基于交叉混沌映射的小波域图像加密算法 [J]. 计算机应用与研究, 2018, 35 (6): 1797-1799, 1811. (Yan Bing, Bai Sen, Liu Bowen, Yang Yi, Guo Hui. Algorithm of image encryption in wavelet domain based on cross chaotic map [J]. Application Research of Computers, 2018, 35 (6): 1797-1799, 1811.)

[6] 张勋才，刘奕杉，崔光照. 基于 DNA 编码和超混沌系统的图像加密算法 [J/OL]. 计算机应用研究, 2019, 36 (4) . (2018-02-07) [2018-02-07]. http://www. arocmag. com/article/02-2019-04-034. html. (Zhang Xuncai, Liu Yishan, Cui Guangzhao. Image encryption algorithm based on DNA encoding and hyper-chaotic system [J/OL]. Application Research of Computers, 2019, 36 (4) . (2018-02-07) [2018-02-07]. http://www. arocmag. com/article/02-2019-04-034. html.)

[7] 柴秀丽，甘志华. 基于超混沌系统的位级自适应彩色图像加密新算法 [J]. 计算机科学, 2016, 43 (4): 133-139. (Chai Xiuli, Gan Zhihua. A novel bit level adaptive color image encryption algorithm based on hyper chaotic system [J]. Computer Science, 2016, 43 (4): 133-139)

[8] 赵佳星，张雪锋. 基于组合混沌系统的时空彩色图像加密算法 [J]. 计算机工程与设计, 2016, 37 (9): 2354-2360. (Zhao Jiaxing, Zhang Xuefeng. Spatiotemporal color image encryption method based on combined chaotic system [J]. Computer Engineering and Design, 2016, 37 (9): 2354-2360.)

[9] 张勇. 混沌数字图像加密 [M]. 北京. 清华大学出版社. 2016: 105. (Zhang Yong. Chaotic digital image cryptosystem [M]. Beijing. tsinghua university press. 2016: 105.)

[10] 何润民，马俊. SHA-256 算法的安全性分析 [J]. 电子设计工程, 2014, 22 (3): 31-33. (He Runmin, Ma Jun. Analysis safety of SHA-256 algorithm [J]. Electronic Design Engineering, 2014, 22 (3): 31-33.)

[11] 王宏达. 一种基于混沌系统的新型图像加密算法 [J]. 光学技术, 2017, 43 (3): 260-266. (Wang Hongda. A novel image encryption algorithm based on chaotic system [J]. Optical Technique, 2017, 43 (3): 260-266.)

[12] Zhu Hegui, Zhao Cheng, Zhang Xiangde. A novel image encryption-compression scheme using hyper-chaos and Chinese remainder theorem [J]. Signal Processing: Image Communication, 2013, 28 (6): 670-680.

[13] 朱淑芹，李俊青，葛广英. 基于一个新的五维离散混沌的快速图像加密算法 [J]. 计算机科学, 2016, s2 (43): 411-416. (Zhu Shuqin, Li Junqing, Ge Guangying. Fast image encryption algorithm based on novel five dimensional discrete chaos. [J]. Computer Science, 2016, s2 (43): 411-416.)

[14] Zhang Miao, Tong Xiaojun. A new algorithm of image compression and encryption based on spatiotemporal cross chaotic system [J]. Multimed Tools Appl, 2014, 71: 1-25.